

UNITED STATES DISTRICT COURT

for the
Middle District of North Carolina

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

The Person of Joseph Schwehm,
Date of Birth 09/15/1990

Case No.

1:20mj87

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

The person of Joseph Schwehm, date of birth 09/15/1990, described in Attachment A.

located in the Middle District of North Carolina, there is now concealed (identify the person or describe the property to be seized):

Evidence of, instrumentalities used in committing, and fruits of the crimes of 18 U.S.C. §§ 2251, 2252A(a)(2)(A), and 2252A(a)(5)(B), all of which are more particularly described in Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. §2251(a)	Production of Child Pornography
18 U.S.C. §2252A(a)	Distribution, Receipt, & Possession of Child Pornography

The application is based on these facts:

See attached Affidavit

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

15/ Marisa Brown
Applicant's signature

Marisa Brown, Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
telephone and e-mail transmission (specify reliable electronic means).

Date:

March 6, 2020

L. Patrick Auld
Judge's signature

City and state: Greensboro, North Carolina

L. Patrick Auld, United States Magistrate Judge
Printed name and title

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

The property to be searched is 10450 Alabaster Drive, Davidson, NC 28036, further described as a double-story house, single family residence. The residence is brick and stone sided with a covered porch. A black rod iron fence encapsulates the back yard of the residence. A paved driveway located on the right side of the residence leads to an attached, covered garage. A mailbox with the numbers "10450" imprinted on the newspaper tube sits at the base of the driveway at Alabaster Drive.



¹ Image taken from Google Maps

The property to be searched includes a 2010 Toyota Corolla, license plate number TPT6899.

The person to be searched is Joseph M. Schwehm, a white male whose date of birth is September 15, 1990, and whose social security number is 226-65-1896. His photograph is included below.



ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2251(a), 2252A(a)(2)(A), 2252A(a)(5)(B), and 2422(b):

1. Computers or storage media that could be used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
 - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user

profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- e. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;
- f. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- g. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- h. records of or information about Internet Protocol addresses used by the COMPUTER;

- i. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses revealing an interest in child exploitation content .
- 3. Routers, modems, and network equipment used to connect computers to the Internet.
- 4. Child pornography, as defined in 18 U.S.C. 2256(8).
- 5. Child erotica.
- 6. The following clothing depicted in child pornography images received or sent by Kik user bluedayguys: male child's red shorts and shirt, male child's stretch boxer shorts, and a solid gray fleece blanket.
- 7. Records, information, and items relating to violations of the statutes described above in the form of:
 - a. Records, information, and items referencing or revealing the occupancy or ownership of 10450 Alabaster Drive, Davidson, NC 28036, including utility and telephone bills, mail envelopes, or addressed correspondence;

- b. Records and information referencing or revealing the use and user of a Kik group titled "Open Minded Parents";
- c. Records and information referencing or revealing the use of the handles/pseudonyms bluedayguys, blueday, Blue Day, or variations thereof, in any online accounts or services;
- d. Records and information revealing sexual activity with or sexual interest in minors, to include conversation via the Internet discussing the grooming of minors for sexual exploitation;
- e. Records and information constituting or revealing membership or participation in groups or services that provide or make accessible child pornography;
- f. Records and information revealing the use and identification of remote computing services such as email accounts or cloud storage; and
- g. Records and information referencing or revealing the sexual exploitation of children and trafficking of child pornography, including correspondence and communication between users of any application, such as Kik Messenger, concerning the advertisement, distribution and production of child pornography.

8. During the course of the search, photographs of the searched premises may be taken to record the condition thereof and/or the location of items therein.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact

discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF NORTH CAROLINA

IN THE MATTER OF THE SEARCH
OF:

THE RESIDENCE, OUTBUILDINGS,
APPURTENANCES, AND VEHICLES
LOCATED AT 10450 ALABASTER
DRIVE, DAVIDSON, NC 28036, AND
THE PERSON OF JOSEPH
SCHWEHM

Case No. 1:20-mj-87

AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR A SEARCH
WARRANT

I, Marisa Brown, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been since May 2019. As such, I am a “federal law enforcement officer” of the United States within the meaning of Rule 41 of the Federal Rules of Criminal Procedure. I am currently assigned to the Charlotte Division, Violent Crimes Against Children Program and am designated to work a variety

of criminal matters, including child sexual exploitation, Internet crimes against children, and human trafficking.

2. My career in law enforcement began as a Staff Operations Specialist with the FBI where I was assigned to support the FBI's mission to combat violent crimes. I was involved in searches, seizures, arrests, and intelligence gathering. I graduated from the FBI Academy as a Special Agent and have received basic and on-the-job training in the investigation of cases involving the sexual exploitation of children. During my career as an FBI Special Agent, I have participated in child pornography and human trafficking investigations. I have participated in the investigation of cases involving the use of computers, cellular devices, and the Internet to commit violations of federal child exploitation laws. I have received training and gained experience in human trafficking and child exploitation investigations, interview and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, and various other criminal laws and procedures relevant to the instant investigation. I have participated in operations targeting underage victims of sex crimes.

3. I am investigating the activities of the Kik username bluedayguys. As will be shown below, there is probable cause to believe that someone using the Kik account bluedayguys has produced child pornography, in violation of 18 U.S.C. §§ 2251(a), and has transported, received, possessed, and distributed child pornography, in violation of 18 U.S.C. 18 U.S.C. §§ 2252A(a)(2)(A) and (a)(5)(B). I submit this Application and Affidavit in support of a search warrant authorizing a search of the property and residence 10450 Alabaster Drive, Davidson, NC 28036, along with a 2010 Toyota Corolla, and the person of Joseph M. Schwehm, as further described in Attachment A. Located within the premises to be searched, I seek to seize evidence, fruits, and instrumentalities of the forgoing criminal violations, which relate to the knowing transportation, receipt, possession and distribution of child pornography. I request authority to search the entire premises, including the residential dwelling, vehicles or boats located on the property, or any outbuildings such as detached garage, sheds or barns. In addition, I request authority to search any computer and computer media located therein where the items specified in Attachment B may be found, and to seize all items listed

in Attachment B as instrumentalities, fruits, and evidence of crime.

4. The statements in this Affidavit are based in part on information provided by FBI undercover employees, other law enforcement entities and on my investigation of this matter. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violation of 18 U.S.C. § 2251 and 2252A are presently located at 10450 Alabaster Drive, Davidson, NC 28036.

STATUTORY AUTHORITY

5. This investigation concerns alleged violations of 18 U.S.C. § 2251 relating to material involved the sexual exploitation of minors.

- a. 18 U.S.C. § 2251(a) makes it a crime for any person who employs, uses, persuades, induces, entices, or coerces any minor to engage in, or who has a minor assist any other person to engage in, or who transports any minor in or affecting interstate or foreign

commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct for the purpose of transmitting a live visual depiction of such conduct.

6. This investigation concerns alleged violations of 18 U.S.C. § 2252A relating to material involving the sexual exploitation of minors.

a. 18 U.S.C. § 2252A(a)(2)(A) prohibits a person from knowingly receiving, distributing or conspiring to receive or distribute any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

b. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing or knowingly accessing with intent to view, or attempting to do so, any material that contains an image of child

pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

DEFINITIONS

7. The following definitions apply to this Affidavit and Attachment B:
- a. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.
 - b. "Child Pornography" includes any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct;

(b) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. See 18 U.S.C. § 2256(8).

- c. “Computer” refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.” See 18 U.S.C. § 1030(e)(1).
- d. “Computer hardware” consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal

and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

- e. "Computer passwords and data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or

“hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

- f. “Computer-related documentation” consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.
- g. “Computer software” is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.
- h. IP Address: The Internet Protocol address (or simply “IP address”) is a unique numeric address used by computers on the Internet.

An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- i. “Minor” means any person under the age of 18 years. *See* 18 U.S.C. § 2256(1).
- j. “Sexually explicit conduct” refers to actual or simulated (a) sexual intercourse (including genital-genital, oral-genital, or oral-anal), whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic areas of any person. *See* 18 U.S.C. § 2256(2)(A).

- k. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).
- l. The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); mechanical form (including, but not limited to, phonograph records, printing, typing); or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital

data files and printouts or readouts from any magnetic, electrical or electronic storage device).

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

8. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers, computer technology, and the Internet have revolutionized the manner in which child pornography is produced and distributed.

9. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

10. Child pornographers can transpose photographic images from a camera into a computer-readable format with a scanner. With digital cameras, the images can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

11. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

12. The Internet affords collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

13. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online

storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

14. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

15. Based on my knowledge, training, and experience, I know that computer storage devices, such as a computer hard drive, can store information for long periods of time. Even when a user deletes information from a device, it can sometimes be recovered with forensics tools. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

16. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

17. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is

available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.

18. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, deleted, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

19. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU).

In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

20. Furthermore, because there is probable cause to believe that the computer and its storage devices are all instrumentalities of crimes, within the meaning of 18 U.S.C. §§ 2251 through 2256, they should all be seized as such.

PROBABLE CAUSE

21. On March 4, 2020, an Online Covert Employee (OCE) was acting in an undercover capacity and entered a private parent KIK group. KIK is an instant messaging application for mobile devices. Upon entering the group, an automatic rules message appeared on the screen stating the following: "Age, Sex, Location & children's ages upon entry; must have a child or step child to be part of the group; This is a group for open minded parents / if your not sure

what that means you are probably in the wrong group; Ask before you PM anyone & be respectful (any issues report to the owner or an admin); Lastly you will need to verify with the Owner or an admin (sit tight and someone will contact you soon and let you know how to verify)."

22. The OCE identified himself as a 33 year-old dad with a daughter in the United States. An administrator of the group, "bluedayguys," sent a message to the OCE asking him to verify. The OCE contacted "bluedayguys" in a private KIK chat and informed "bluedayguys" that he was the father of an 8-year-old girl. "bluedayguys" stated "Just need a live pic and proof you're a parent." The OCE sent "bluedayguys" an image of his purported daughter and an image of a pair of children's panties. "Bluedayguys," responded to the OCE, "very nice," and "you active with her."

23. The OCE told "bluedayguys" the OCE was sexually active with his purported daughter while she sleeps. "Bluedayguys" informed the OCE that his girlfriend has a 6 year-old son that "bluedayguys" is sexually active with. "Bluedayguys" told the OCE that he touches and sucks the child. During the

course of the chat, "bluedayguys" sent the following pictures of the 6 year-old boy:

- a. Picture 1: A clothed image of a prepubescent boy wearing a red shirt and red shorts. His face is visible in the photo.
- b. Picture 2: An image of a person pulling up a solid gray fleece-type blanket and exposing what appears to be a prepubescent child sleeping. The focus of the image is on his crotch and he is wearing shorts or underwear. A cat can be seen lying next to the child.
- c. Picture 3: An image of an adult hand holding the wrist of a prepubescent child. The child's hand is touching the adult's bare penis.
- d. Picture 4: An image of an adult placing his penis on a prepubescent boy's face while the child is sleeping. The same blanket as described in picture #2 is visible in this image.
- e. Picture 5: An image of what appears to be a prepubescent child. This child is wearing some type of stretch boxers or shorts.

24. During the course of the chat, "bluedayguys" told the OCE that his girlfriend has no clue "bluedayguys" abuses her son. "bluedayguys" stated that he works in construction and resides in North Carolina. During the course of the chat the OCE asked "bluedayguys" if "bluedayguys" could take a live picture of the blanket and cat that was seen in the images sent by "bluedayguys" for the purpose of verifying that the images were produced by "bluedayguys." "bluedayguys" stated that he was currently at work but would send the requested images later that evening upon returning home from work.

25. On March 4, 2020, at approximately 7:05pm EST "bluedayguys" sent the OCE a live image of a blanket and a live image of a cat. The cat appears to be the same cat as seen in the photo described above. The blanket appears to be similar as the blanket described in a separate photo.

26. On March 5, 2020 an emergency disclosure request (EDR) was sent to Kik for subscriber identification information and IP access logs associated with this username. Kik's EDR response provided a display name of Blue Day, unconfirmed email address of bluedayguy@gmail.com, and IP access logs from approximately 2/4/2020 - 3/5/2020. A review of the IP logs yielded a

combination of Spectrum (Charter Communications) and Verizon Wireless IPs. The IP address 65.184.68.215 was found to be associated with the Kik account "bluedayguys".

27. On March 5, 2020 an EDR was submitted to Charter Communications/Spectrum for subscriber information for IP address 65.184.68.215 on 3/5/2020 at 10:24:35 UTC. Charter Communications/Spectrum provided a verbal response that the subscriber of this IP address was Margaret Wojciechowicz, 10450 Alabaster Drive, Davidson, NC 28036.

28. A review of open source information and North Carolina Department of Motor Vehicle (DMV) records indicated current residents of 10450 Alabaster Drive, Davidson, NC 28036 are Margaret Wojciechowicz and Joseph M. Schwehm. A review of the DMV photo of Margaret Wojciechowicz was consistent to the photograph the subject sent the OCE of his supposed girlfriend. A review of DMV records indicated that Joseph M. Schwehm, birthdate 09/15/1990, is the registered owner of a 2010 Toyota Corolla with the license plate number of TPT6899.

29. A review of Margaret Wojciechowicz's open source information indicated she was previously married to and lived at the 10450 Alabaster Drive address with Robert Wojciechowicz. A review of Robert Wojciechowicz's social media profile on Facebook indicated Robert Wojciechowicz is the father of the victim child identified in the photographs, and that the victim child resides at 10450 Alabaster Drive.

CONCLUSION

30. Based on the aforementioned factual information, your Affiant respectfully submits that there is probable cause to believe that an individual at the residence described above is involved in the production, transportation, receipt, possession and distribution of child pornography. Your Affiant respectfully submits that there is probable cause to believe that an individual in the residence described above has violated 18 U.S.C. §§ 2251, and 18 U.S.C. §§ 2252A. Additionally, there is probable cause to believe that evidence of criminal offenses, namely, violations of 18 U.S.C. §§ 2251(a), and 18 U.S.C. §§ 2252A(a)(2)(A) and (a)(5)(B), is located in the residence described in Attachment A, and this evidence, listed in Attachment B to this Affidavit,

which is incorporated herein by reference, is contraband, the fruits of crime, or things otherwise criminally possessed, or property which is or has been used as the means of committing the foregoing offenses.

31. Your Affiant, therefore, respectfully requests that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.

REQUEST FOR SEALING

32. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other online criminals as they deem appropriate, i.e.,

post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,

15 / Marisa Brown *by LPA*

Marisa Brown

Special Agent

Federal Bureau of Investigation

Attested

~~Subscribed~~ and sworn to before me
on March 06, 2020 *by telephone after email transmission*

[Signature]

UNITED STATES MAGISTRATE JUDGE